NSI code of practice for design, installation and maintenance of CCTV surveillance systems

NCP 104.3

November 2017

National Security Inspectorate
Sentinel House,
5 Reform Road
Maidenhead
SL6 8BY
Website: nsi.org.uk

Contents

In this document, material (such as guidelines, information, recommendations, advice) that does not form a mandatory requirement of this code of practice is shown in italics

Introduction

This code of practice is based on the format of "BS EN 62676-4:2015 -Video surveillance systems for use in security applications. Application guidelines".

This code of practice has been laid out to enable security companies to follow a logical process through the development and delivery of a video surveillance system (VSS) in order to meet a user's requirements. Relevant clauses in BS EN 62676-4 have been annotated against clauses within this code of practice for cross referencing purposes.

The use of VSS, more commonly known as CCTV (Closed Circuit Television), as a means to provide a safety or security function has increased significantly in recent years. Advances in technology and a reduction in product cost has led to an increase in their use in both the residential and commercial sectors of the market. Additionally modern communication technologies have been able to deliver high quality images to enable the remote monitoring of CCTV systems, using personal mobile devices and/or third party monitoring centres, to be a standard requirement for many users.

To ensure that a CCTV system will meet the user's needs, an information gathering process has to be carried out to enable the designer to understand the user's expectations prior to starting the design and installation process. During the design and installation process, it may be necessary review and revise the requirements and proposed solution with the user to ensure the delivered system achieves its aims and objectives. Failure to engage with the user may lead to expectations not being met and subsequently the system may not provide the information and/or evidence it was intended to capture.

When installed, systems will need some element of maintenance to ensure they continue to function correctly and meet the user's requirements. Although changes in technology have potentially decreased the need for the maintenance of system hardware, the increased use of software and firmware, either embedded in system components or used in application and operating systems, offers different challenges in maintaining the system's integrity. These have increased the system's vulnerability to threats from hacking and malware, potentially allowing components to be used as a means to steal information held on the surveillance system or as a vector to disrupt other connected networks. Therefore the designer needs to consider how these threats are to be initially mitigated and, once the system is installed, how these threats will be managed as part of the ongoing maintenance regime.

1 Scope

This Code of Practice applies to NSI NACOSS Gold and NSI Systems Silver approved companies and specifies requirements for the design, installation, commissioning and maintenance of continuous and detector activated CCTV surveillance systems.

Typical examples are: perimeter surveillance, access control, property protection and automatic number plate recognition. Examples of events that may be monitored by these applications include hold-up, theft, sabotage, vandalism, hazards and evacuation.

This Code of Practice does not recommend the extent or degree of the protection in the security application, nor does it necessarily cover all the requirements for any other surveillance applications.

CCTV that is used purely for process control and/or purely for video door entry systems falls outside the scope of this Code of Practice.

NSI NACOSS Gold and Systems Silver approved companies must comply with:

- This Code of Practice (NCP 104); or
- BS 8418

Remotely monitored detector activated CCTV systems developed in accordance with BS 8418 fall outside of the scope of this Code of Practice.

NCP 104 is based on the format of BS EN 62676-4:2015. However, significant elements regarding the grading of CCTV systems and use of specific image test requirements have been omitted and therefore compliance to NCP 104 cannot be used to claim compliance to the BS EN 62676 series of documents.

Throughout the document, requirements are written in roman, i.e., upright type, and the auxiliary verb in these cases is 'must'. Where a requirement is relevant to the risk assessment, site survey, user requirement, system design, installation, test, commissioning, handover, documentation and/or maintenance of the system it is mandatory to apply these requirements to ensure compliance with this code of practice.

Notes and recommendations are written in italics and, where relevant, the auxiliary verbs are 'should, can, may or will'. These notes and recommendations are included as guidance to assist in the risk assessment, site survey, user requirement, system design, installation, test, commissioning, handover, documentation and/or maintenance of the system.

2 References

"BS EN 62676-4:2015 Video surveillance systems for use in security applications. Application guidelines".

References to clauses in BS EN 62676-4:2015 have been included in the relevant clause numbers in this document for cross reference purposes and are not intended to require or imply that the full provisions of every clause of BS EN 62676-4 need to be met.

3 Terms and definitions and abbreviations

3.1 Terms and definitions

3.1.1 CCTV surveillance system

A security system using a combination of hardware and software to provide the images (and audio where required) necessary to perform a safety or security function.

3.1.2 Customer

An individual or organisation entering into a contract with a security company.

3.1.3 Operational period

A time period over which all or part of the CCTV surveillance system is required to function to meet the user requirement.

3.1.4 Security company

An organisation contracted to provide the design, installation and/or maintenance of a CCTV surveillance system.

3.1.5 System owner

An individual or organisation responsible for the control and management of a CCTV surveillance system.

3.1.6 Operator

An individual trained and authorised to operate all or part of the CCTV surveillance system.

3.1.7 User

A customer, system owner or other organisation responsible for defining the scope of the CCTV surveillance system.

3.1.8 User requirement

A document which defines the functions of the CCTV surveillance system.

Note: May be referred to as the operational requirement.

3.2 Abbreviations

BID	Beam Interrupt Device
CCTV	Closed Circuit Television
ICO	Information Commissioner's Office
LAN	Local Area Network
LiDAR	Light Detection and Ranging
MJPEG	Motion Joint Photographic Experts Group
MPEG	Motion Pictures Expert Group
PIR	Passive Infrared
PoE	Power over Ethernet
PTZ	Pan Tilt Zoom
SDS	System Design Specification
SSO	Single Sign On
TLS	Transport Layer Security
UR	User Requirement
URN	Unique Reference Number
UTC	Universal Time Clock
VCA	Video Content Analysis
VLAN	Virtual Local Area Network
VSS	Video Surveillance System
WAN	Wide Area Network

4 Risk assessment *(BS EN 62676-4 Clause 4.2)*

A risk assessment must be carried out and documented.

A user would normally carry out the risk assessment and this would be the basis of the User Requirement (UR) (see Clause 6). However, you would complete and document the risk assessment where the user is unsure how to undertake a risk assessment and/or the risk assessment is considered to be incomplete.

The risk assessment can be produced as a standalone document (see Appendix A) or it can be included as part of the UR, site survey or system design specification (SDS).

During the risk assessment consideration must also be given to the threat of the CCTV system being reduced in capability or disabled through accidental or malicious actions. You must mitigate or identify to the customer any risks to the continuing operation of the system.

Risks may include vandalism of cables and cameras, loss of power or remote access, loss of illumination sources and unauthorised access to the system's operating systems, applications or networks from internal or external sources.

4.1 Considerations

The following must be considered as part of the risk assessment:

4.1.1 Targets

For example: personal attack, theft of goods, cash, data, intellectual property, vandalism, anti-social behaviour, environmental risks to individuals - monitor for crowd control and staff safety, identify/recognise individuals for control of entry, detect and observe anti-social behaviour and interference with pets, livestock and wild animals.

4.1.2 Location

For example: urban, suburban or rural area, prevailing environmental conditions, existing security arrangements, property construction.

4.1.3 Occupancy

For example: hours of occupancy of areas where risks have been identified, public access to risk areas.

4.1.4 History of criminality in area

For example: prevalence of any particular criminal activities, methods of attack.

5 Site survey *(BS EN 62676-4 Clause 4.4)*

A site survey of the proposed system location must be carried out and documented either as part of the SDS or within a separate document. See Appendix B.

The site survey may be carried out after the UR has been produced (see Clause 6).

Where you carry out the site survey, the following information must be documented, where applicable:

- The date, time and location of the survey.
- Drawings and/or photographs and/or notes of the proposed location, including details of target and risk locations.

- Notes on the approximate distances to target and risk areas (to aid camera and lens selection).
- Candidate locations for system components.
- Details of illumination.
- Local environmental concerns that may affect the design (foliage, vehicle parking, adjacent public and private property boundaries, and so on).
- Any restriction on access and requirements for civil works; for example, power, communications, cable routing, and so on.

Where another party carries out the site survey, details of the organisation/individual who carried out the survey and a reference to the survey document must be included in the SDS.

Where it has not been possible or it is not considered either practicable or necessary to carry out a site survey, (for example the system design has been provided by the user or where the property has not been built) this fact and any limitations that may affect the design of the system, (for example, expected lux levels, proximity of adjacent properties, changes in internal layout) must be made in clear in the system design documentation.

6 User requirement *(BS EN 62676-4 Clause 5)*

The UR must be developed either by the user or by you in discussion with the user.

Where agreed with the customer, the UR may be a separate document or may be included within the SDS.

The UR must, at a minimum, include a statement that covers the elements of the following clauses necessary to the design of the system:

6.1 Basic objectives and functions

A statement detailing the intended purpose of the system and what the deployment of the system is expected to achieve.

6.2 Surveillance areas

A general description of the area(s) under surveillance.

6.3 Activities to be captured

What is the intended target of surveillance at each location?

What is the target's likely speed/direction?

Required to enable frame rate, shutter speed and functional camera performance to be correctly specified.

What is the purpose of the images captured at each location (See Appendix C)?

To enable the understanding of terms, users should be provided with a copy of Appendix C prior to developing the UR.

Image categories chosen should reflect the detail in which the target is to be seen. Should an observer need to see some characteristic details of the individual, such as distinctive clothing, whilst the view is required to be sufficiently wide enough to allow activity surrounding an incident to be monitored then the requirement is to "observe" not "monitor" or "detect". Failure to apply the various image categories correctly to the expected scenario will lead to a poorly designed system that does not meet the user's expectations.

What are the requirements for detecting the movement of targets?

PIR detectors, BIDs, LiDAR or VCA may be configured to initiate a function or response for example start recording, cue a functional camera, turn on illumination and so on.

6.4 System/image performance

What are the requirements for the system to be capable of detecting and/or tracking targets (manually, automatically or both)?

What image quality for the live viewing, playback and export of images is required?

What alerts (messages) and alarms are required on the system?

Where a requirement is identified in the UR to raise visual or audible alerts and alarms, this may require a trigger, for example a system input from a detector or video analytics engine, to be integrated into the system.

6.5 Operational periods

When will parts or all of the system be used (24/7, quiet hours, busy hours)?

6.6 Environmental conditions

What are the prevailing weather and/or atmospheric conditions on site?

What illumination exists in the target area(s) (type of illumination, hours of operation, lux levels)?

Surveyors should use lux meters that have sufficient range and sensitivity to measure all expected light levels in the environment where the system is expected to provide coverage.

What potential obstructions to camera views exist (foliage, traffic, stock, etc.) or may exist due to seasonal variations?

What local environmental issues, such as illumination (manmade/sunrise/sunset) and wildlife (insects, game, vermin) exist that may obscure camera views or cause detectors to malfunction (may be identified in the site survey)?

Environmental risks may include flammable, atmospheric, intrinsic safety, chemical, radiological, electrical noise, high lightning risk and other higher risk environments.

6.7 Resilience

What are the requirements to protect or detect tampering of the system?

What are the requirements to protect part or all of the system from power failures?

What are the requirements to protect against unauthorised access to systems and software (applications and operating systems)?

What are the requirements to protect internal and external network connections?

The information above may be required for interoperability, capacity and security purposes.

Where a mobile device, such as a phone or tablet, is intended to be used to connect to the system, the user should be made aware of the need to ensure access to the mobile device's operating system and applications are restricted by the use of strong authentication, such as complex passwords, gestures or biometrics.

6.8 Monitoring, record and store

Where will the system be monitored (local, remote, both)?

When will the system be monitored (continually/occasionally/in the event of an alarm or trigger/after an incident)?

Who monitors the system (individual operator, customer's family or staff, contracted monitoring centre)?

What images are recorded (continuous, defined periods before and after incidents/activations)?

How long do images need to be retained for?

Where will the images be stored (locally/remotely)?

Where the system is to be monitored using mobile devices, the user should be advised of limitations that may exist in the ability of the system to provide the level of image detail expected due to screen size or communications capability.

6.9 Export

Have specific media and file format(s) been identified for exported images and is there a requirement to have a media player embedded in or provided with any exported media?

Where no specific export format is identified by the user, systems should be configured to export data in an open file format.

6.10 Operational response

What, if any, operational responses are to be put in place following incidents detected or reported by the system?

Full details of any operational responses may be included in a separate document

6.11 Operator requirements

How many workstations (concurrent operators) will be required to carry out monitoring and data manipulation tasks?

There may be a requirement to assess operator workload with regard to the monitoring of live events and alarms.

6.12 Training

What operator training will be required to manage the system?

Depending on the complexity of the system, this may range from basic operator training to a contracting out of training to a specialised training organisation.

Training needs can be identified in the system design documentation.

6.13 System expansion

What requirements might there be for system expansion? What are the requirements to integrate the system with other systems, CCTV or otherwise?

The system design documentation should include details of unused system capacity, such as cameras, triggers and media.

6.14 Audio

What are the requirements for any broadcast or interactive audio associated with the system?

What are the requirements for one-way or bi-directional audio, and will this be simplex or duplex?

6.15 Limitations of surveillance

Legal issues that may affect the installation and operation of the system (see Clause 7.1).

7 System design

The system design must address all the requirements captured in the UR taking into account any constraints imposed by limitations identified in the site survey.

The system design should consider how areas where operating temperatures or environmental conditions that are harsh may need special attention.

Where there is a high risk of lightning strike, suitable protection should be either identified to the customer or provided.

You must document the system design in a fully documented SDS. The SDS must have a unique reference number and a means to identify revisions caused by any design changes.

During the system design process, you must discuss with the user any limitations identified which prevent the UR from being met in order to agree any resolutions. Any changes to the UR and any subsequent changes to the system design must be documented.

The agreed system design must be fully documented in a SDS which must be signed off by the customer or the customer's representative.

Acceptance may be in the form of an email or response to a contract document as long as these contain a reference to the SDS.

During the tendering process for a contract, a précis of the system design may be provided to the customer in order to provide an overview of the solution to be provided.

Consideration must be given to the capability of the system to meet the UR when integrating system components from different applications, for example, intruder systems, access control systems and so on.

Consideration of environmental factors associated with the system components should be assessed (low power, disposal of consumables, reuse of media, use of hazardous substances, and so on).

7.1 Legislation and standards

The SDS must draw the customer's attention to the Data Protection Act and the information available from the Information Commissioner's Office.

Data Protection Act (DPA) 1998[1]

All CCTV systems are potentially subject to the requirements of the Data Protection Act. To assist designers, operators and owners of CCTV systems, the Information Commissioner's Office (ICO) has published a number of documents to provide guidance on the design, installation and operation of CCTV systems including information on data retention periods, the requirements for signage and the use of audio recording. To obtain more information, please go to https://ico.org.uk/

Protection of Freedoms Act (POFA) 2012

Relevant authorities, as defined in the POFA, using CCTV for surveillance of public space are required to comply with this legislation. To assist relevant authorities to comply with this legislation, the Home Office has produced guidance in the form of a Surveillance Camera Code of Practice giving 12 Guiding Principles to be followed when designing, installing and operating public space surveillance camera systems. To obtain more information, please go to https://www.gov.uk/government/organisations/surveillance-camera-commissioner

Private Security Industry Act (PSIA) 2001

Attention is drawn to the Security Industry Authority's (SIA's) requirements for the licensing of individuals engaged in public space CCTV surveillance and in other security related activities (see www.the-sia.org.uk) and see also the British Standard BS 7958 Closed circuit television (CCTV) - Management and operation - Code of Practice.

When installing CCTV systems and entering into contracts with customers to provide CCTV monitoring services you should ensure that, in relevant circumstances, you use monitoring companies where the individuals providing the CCTV monitoring service hold the appropriate SIA licenses.

Similarly, where customers are likely to enter into their own contracts with third-party providers of monitoring services, you should advise customers to ensure that, where relevant, they use monitoring companies where the individuals providing the CCTV monitoring service hold the appropriate SIA licenses.

We remind you that, under NSI rules and criteria for approval, you must use monitoring centres that hold NSI ARC Gold approval for the monitoring of CCTV systems or an ARC which holds an equivalent third party certification to a standard acceptable to NSI.

[1] The General Data Protection Regulations (GDPR), which will replace the Data Protection Act 1998 are due to come into force in the UK from 25 May 2018. Further information on the requirements of the GDPR in relation to CCTV systems will be published by the Information Commissioner's Office at the following website: www.ico.org.uk.

Town & Country Planning Act (TCPA) 1990

The Town and Country Planning (General Permitted Development) (England) Order 2015 Schedule 2 Part 2 Class places restrictions on the siting and quantity of CCTV cameras deployed on the outside of buildings. Designers should make themselves aware of these requirements as they may impact on the design and operation of the CCTV system.

Clear Neighbourhoods and Environment Act (CNEA) 2005

Designers should be aware that the Clean Neighbourhoods and Environment Act provides for local authorities to enforce restrictions on sources of lighting or noise pollution. Consideration should therefore be given to ensuring any additional illumination or audio broadcast deployed as part of the system does not become subject to a light or noise pollution order.

7.2 Site Plan *(BS EN 62676-4 Clause 6.6)*

A site plan must be included in the SDS which details the locations of interest (risk areas and targets) and key system components, including: cameras (including field of view and distance to risk areas and targets), detectors (including range and coverage), illumination (existing and additional) and control equipment (monitor and record).

The site plan may be a line diagram or a marked up photographic/video representation of the proposed location detailing the required information as either graphics or as a written description.

7.3 Camera equipment *(BS EN 62676-4 Clause 6.2, 6.3 & 6.4)*

Lens and camera combinations must be selected to ensure resolution, object size, field of view and illumination performance meets the UR.

7.4 Functional cameras (PTZ) *(BS EN 62676-4 Clause 6.4.2)*

Where identified in the UR, functional cameras must have a home location and must return automatically to this position after a predefined period.

If pre-set positions have been identified in the UR, these must be annotated on the site plan.

The functional camera must be capable of tracking the fastest expected target.

Tracking of targets can be carried out either manually or automatically.

7.5 Equipment housings *(BS EN 62676-4 Clause 6.5)*

All equipment and associated housings must be suitable for the expected environmental conditions.

7.6 Field of view/object size *(BS EN 62676-4 Clauses 6.7 & 6.8 & Table 3)*

The quality of the image on the display must have sufficient detail to meet the UR.

Guidance on image height in relation to display resolution are included in Appendix C.

In digital imaging, it is important to understand the relationship between the camera resolution and the screen display resolution. If the camera resolution is not equal to the display resolution or vice versa, the displayed scene may not show the expected level of detail.

For target images where the requirement is to identify or recognise individuals, cameras should be placed as close to head height as possible. Where the requirement is to observe, detect or monitor, cameras should be mounted at a height that achieves the required coverage.

When setting up a camera field of view, it is also important to consider other environmental or scene specific content, for example:

- *Foliage: Growth of or seasonal variations in foliage may obscure views;*
- *Illumination: spot lighting from external light sources, illumination located adjacent to the camera causing poor image quality due to flying insects, snow, rain, and so on. causing glare and reflections and time controlled lighting may affect the view;*
- *Sunlight: depending on time of day and seasonal variations, the position of the sun could produce glare or provide poor illumination conditions such as backlighting the target;*
- *Reflections: windows, buildings, water or any other reflective objects can result in poor or excessive illumination conditions and may degrade the image;*
- *Street furniture/signage: temporary or new permanent structures such as signs or other buildings may obscure views;*
- *Scene activity: if a specific image is required, ensure that other scene activity will not obscure the target.*

7.7 Detectors, video analysis, triggers, alerts and thermal imaging

Detection areas must be within the associated cameras field of view.

Detectors must be able to cover the area where targets are required to be detected.

Detectors must be positioned so that activity outside of the target area does not cause activations.

Where there is the possibility of detectors being activated outside of the camera coverage area, the user should be informed.

Detectors must be selected and positioned so that they are not affected by the rising and setting of the sun.

Where video analysis is used to provide detection, sufficient illumination must be provided so that detection in all bounded areas, tripwires, etc., function correctly throughout the operational period.

Triggers and alerts generated by detectors and video analysis must meet the requirements and/or responses identified in the UR.

Thermal imaging devices

Thermal imagers can be used as part of a CCTV system, where operational ranges greater than traditional visible and infrared illuminated cameras are required. Thermal imagers use the heat radiated from the object, as opposed to the light reflected from its surface, to form an image. Thermal imagers can be used to determine the class (vehicle, person, animal) of a target but will not allow an operator to identify the person, or the colour of a vehicle.

The object classifications which are relevant to thermal imagers "DRI" (Detection, Recognition, Identification) are in terms of the number of pixels required on the object to make an accurate assessment and may be specified on equipment in orders of distance, for example x miles or kilometres.

- *Detection: ability to distinguish an object from the background*
- *Recognition: ability to classify the object class (animal, human, vehicle, boat)*
- *Identification: ability to describe the object in details (a man with a hat, a deer, a Jeep)*

These should not be confused with the image categories used for conventional CCTV images (see Appendix C).

Where thermal imaging is used as part of the system design the DRI category and range should be stated in the UR and specified in the SDS.

7.8 Illumination *(BS EN 62676-4 Clause 6.9)*

Existing illumination must be assessed for levels, direction, spectral content and hours of operation.

Designers should be aware that whilst camera manufacturers may claim their products will work down to extremely low lux levels, the cameras may not be able to achieve the necessary level of detail required by the UR at these levels of illumination. This is especially valid when there is a need to capture images of moving objects. Failure to

identify these limitations at the design stage may result in the system being unable to achieve a satisfactory level of performance over the systems operational period.

Requirements for additional illumination must be determined.

The UR should address the questions of what does the user want to see, when does the user want to see it and in what detail. The illumination available or specified should meet these requirements.

During the design process, consideration should also be given to the existence of other sources of external illumination such as sunlight, reflections from buildings or large bodies of water, car lights, and so on, that may affect the quality of images.

Typical illumination levels (in lux)	
Moonless; overcast night sky	0.0001
Moonless; clear night sky	0.001
Quarter moon on cloudless night	0.01
Deep twilight	1
Twilight	10
Well lit main road	30
Stairs/passages	60
Offices/Retail Store	500/750
Daylight	10 000 / 25 000
Full sunlight	32 000 / 130 000

7.9 Video/audio performance *(BS EN 62676-4 Clause 9.1)*

Configuration settings that have an impact on the quality of images must be set to ensure the UR is met.

Scenes containing rapidly changing light and colour detail may be degraded by the use of high compressions rates or low bit rates therefore settings should be appropriate to the scene content. As this may not be apparent until the system is tested, some degree of flexibility should be allowed in the system design.

The format in which images are transmitted, stored and exported from the system must be selected after discussion with any stakeholders.

Image quality tests for live, recorded and exported views must be defined within the test and commission documentation to ensure the system can meet the UR.

Image quality tests may consist of live simulations, static images or objective tests using test targets. Details of test methodologies and example test targets are available in BS EN 62676-4:2015 Appendix B and C.

7.10 Video frame rate *(BS EN 62676-4 Clause 9.2)*

The required frame rate must be determined for each individual camera view.

Consideration should also be given to camera shutter speed as this may affect the image quality of moving targets and the level of illumination required, that is, if a fast shutter speed is required to achieve good quality images, the target area may need higher levels of illumination.

7.11 Video resolution *(BS EN 62676-4 Clause 9.3)*

Camera video resolution must be selected to achieve the level of detail and coverage identified in the UR.

For example, if the image category is observe and a low resolution format is selected, the image will have to be closely framed to achieve the necessary detail which may, in turn, compromise any understanding of the context in which the images are viewed.

The resolution format should be able to achieve the level of detail needed to fulfil the UR without using digital zoom.

7.12 Storage *(BS EN 62676-4 Clause 10)*

The total system storage requirements must be estimated before a system is installed so that appropriate memory capacity can be specified.

A general equation to assist in the calculation of storage capacity is given in BS EN 62676-4:2015 Clause 10.

7.13 Data compression *(BS EN 62676-4 Clause 11.1)*

Standard publicly available compression algorithms must be used.

Archived data should not be subject to further lossy compression as this may affect the quality of video playback and export. Any compression process that prevents data being restored to its original state is considered to be lossy, for example MPEG and MJPEG.

7.14 Encryption *(BS EN 62676-4 Clause 11.2)*

Consideration must be given to the need to encrypt data at rest and data in transit.

Advice on the use of encryption can be found in the following document issued by the Information Commissioners Office (ICO):

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Where data contains methods for ensuring that changes to the data may be detected, they may not alter the compressed image or metadata information.

7.15 Metadata *(BS EN 62676-4 Clause 11.3)*

The format of the video files must allow the size and aspect ratio of each image to be determined.

For video without audio, the time stamp must have a resolution of no less than one second.

Where both video and audio are present, the time stamps must have sufficient resolution to permit synchronised playback of the audio-visual streams.

Where there is a requirement to maintain an accurate system time, this may be provided by the use of a network time source or the provision of instructions to the user on how to manually update the system time.

System time must auto update for changes between any daylight saving offsets and UTC unless otherwise specified.

Requirements for additional metadata (for example geo-data, floor level, VCA, PTZ positions, etc.) must be stated in the UR.

7.16 Image enhancements *(BS EN 62676-4 Clause 11.5)*

Image enhancement tools must not change the original recording.

Where an enhanced image is exported, an audit trail documenting changes to the original image must exist.

7.17 Image export *(BS EN 62676-4 Clause 11.6)*

Data exported from a recorder must have no loss of individual frame quality, change of frame rate or audio quality.

There should be no duplication or loss of frames in the export process.

The system must not apply any format conversion or further compression to the exported images.

Original metadata and authentication signatures must be exported with the images.

The system must have the capability to export of images from selected cameras within defined time periods.

Simultaneous export and recording must be possible without affecting the performance of the system except on systems that require removal of the primary storage media for export purposes.

The export method of the system must be appropriate to the capacity of the system and its expected use.

Removable solid state memory should be sufficient for most export requirements. Requirements for specific media format types should be identified in the UR.

The system must display an estimated time to complete the export of the requested data.

If proprietary software is required to play back exported images then this must be provided with the images.

Where the user has no preference of export format an open format file, such as .avi or .mp4, may be used.

7.18 Displays *(BS EN 62676-4 Clause 7.1 & 7.2)*

Monitors and other viewing devices must be selected and positioned to meet the requirements of the operator's task(s).

Display resolution should be selected to match the camera and resultant video resolution although in some circumstances lower resolution displays may be required to meet a specific need.

7.19 Network and transmission equipment *(BS EN 62676-4 Clause 8)*

The system designer must select the most suitable internal (LAN) and external (WAN) communications infrastructure.

Where you are responsible for the provision of the network, the network must be designed to ensure data is not lost or corrupted during transmission and that images presented for viewing and storage are not subject to any jitter or delay that may affect the UR.

Network requirements must be stated in the SDS for all external connectivity and shared networks.

Network and transmission equipment includes cameras, switches (including PoE switches), routers, firewalls, network termination equipment, external digital and analogue interfaces and cabling providing connectivity to/from a video recorder as part of an internal network and/or as part of the connectivity to an external communications service provider or network.

If sharing a network with other applications and devices consideration should be given to implementing VLANs, quality of service management and end point security.

7.20 Network security

Suitable physical and technical security measures must be put in place to prevent unauthorised access to the system.

Access to all system components, applications and operating systems from internal access points must be restricted to authorised individuals or processes by the use of authentication protocols and access controls.

External access to the network must be restricted to authorised individuals and processes by the use of suitably configured firewalls and/or routers and bridges and/or proxy servers, authentication protocols and access controls.

At a minimum, vulnerabilities in the following areas should be assessed and mitigated or managed [2]:

Boundary firewalls and internet gateways

Security of configuration

Access control measures

Malware protection

Patch management

The capability of all system products should be assessed to ensure these can be made secure against malicious attacks. For example:

Camera security capabilities: TLS communications, detailed audit logs, IEEE 802.1x authentication, enhanced security mode, complex password enforcement, protocol control, security configuration page.

Recording platform security capabilities: TLS communications, detailed audit logs, archive and failover features, camera tamper detection, protected camera LAN, SHA-2 certificates, Active Directory Integration.

Access control security capabilities: TLS communications, detailed audit logs, archive and failover features, login through Windows SSO, highly customizable access control, Denial of Service Protection, encrypted database communication.

Installers should also consider penetration testing of the system if specific security concerns are raised during the risk assessment.

Where known vulnerabilities exist on a system which cannot be mitigated by technical measures, these must be identified and discussed with the system owner.

[2] https://www.cyberaware.gov.uk/cyberessentials/files/requirements.pdf

7.21 Tamper *(BS EN 62676-4 Clause 6.11)*

Cameras must be installed in such a manner to reduce the opportunity to change the field of view of the camera and access cabling.

Where a specific risk of tamper or vandalism has been identified in the UR, cameras should be of a vandal resistance design, be enclosed in a suitably secure housing or placed in a location where access is restricted.

When designing a perimeter security system, consideration should be given to ensuring that each camera is observed by at least one other camera, offering mutual protection.

Where identified in the UR, the system must be capable of detecting signal loss, the obscuration of views and blinding.

Centrally located components, such as record, store, control and network equipment, must be installed in suitably secure locations to protect them from tampering or be provided with means to detect and notify operators/system owners when tampered.

The user should be advised to ensure physical access controls are in place to prevent unauthorised access to the secure location.

7.22 Backup power supplies *(BS EN 62676-4 Clause 12.8)*

Uninterruptible power supplies (UPS) must be provided to those system components necessary to support specific functions identified in the UR.

Consideration should be given to the provision of UPS to system components that may not revert to full operation following a mains restore.

Where a UPS is to be installed, the power consumption of the equipment must be calculated for the purposes of determining the UPS requirements.

7.23 System integration *(BS EN 62676-4 Clause 6.12)*

Integration must not have a detrimental effect on connected systems or host networks.

7.24 Audio

Installed audio must be clearly audible without undue distortion and within the area of coverage of the relevant detectors/cameras as indicated in the system design.

Audio recording should only be carried out if it can be justified as being absolutely necessary and is in accordance with all applicable legislation.

Consideration should be given to day/night audio settings as levels may differ significantly.

7.25 Control rooms *(BS EN 62676-4 Clause 12.1)*

Where there is a requirement for live viewing, camera control or system management tasks, a control room must be specified to house these functions.

A 'control room' can be a single workstation or a large operations centre.

7.26 Operator workstations *(BS EN 62676-4 Clause 12.2)*

The number of camera views presented to an operator must be decided in the system design phase.

There should be the capability to manage the number of camera views presented to the operator.

Images must be presented to the operator at a size sufficient to allow them to undertake the viewing tasks.

For the selection of the screen size, the distance between the display and operator is the primary factor. The general rule is that the viewing distance should be between 3 to 5 times the size of the screen's diagonal.

The operator must be positioned so that they are able to clearly view the information on the display.

Control desks should be ergonomically designed with particular attention being paid to siting of monitors in order to avoid reflections from extraneous light sources on the display screens.

Workstations must be suitably protected from unauthorised use, either by physical or application access control.

7.27 Cabling

Where risks of mechanical damage are identified, cables must be protected by the use suitable conduit, trunking or armour.

Where specific risks of malicious damage are identified in the UR, cables must be protected by suitable means.

Cables types selected must meet manufacturer's recommendations and be suitable for the environment in which they are installed.

Environmental conditions such as dampness, excessive heat, electrical noise, risk of corrosion, mechanical or chemical damage and any requirement to run cables underground or externally should be taken into account in determining the type of cable and degree of protection required for cable runs.

7.28 Supporting structures

Where masts, towers, brackets and supports are used to mount system components, these must be capable of supporting the weight of the component plus any cabling and remain stable and secure during expected climactic conditions (wind and snow).

Where necessary anti-climb measures should be taken to prevent access to system components.

7.29 Training *(BS EN 62676-4 Clause 5.3.15)*

The SDS must include details of the training to be provided, who is to receive the training and when.

For small systems operator training may be provided as part of the handover process. For larger or more complex systems or for groups of operators, training may need to be a formal process which can be carried out in agreement with the customer.

7.30 Maintenance *(BS EN 62676-4 Clause 16.3)*

An assessment of the type and frequency of preventive maintenance must be included in the SDS to take into account installer and manufacturer's recommendations and any specific environmental or operational considerations.

An assessment of the ongoing requirements to maintain the integrity of the system's network security must be carried out and documented in the SDS.

Where this includes the need to maintain licenses and implement patches and updates on the systems software and firmware, this should be carried out annually with recommendations that 'critical' patches and updates be implemented out of normal maintenance periods.

8 Installation

8.1 General *(BS EN 62676-4 Clause 15.2)*

Where site conditions or the risk assessment have changed, the UR and/or the SDS must be revisited to ensure the intended system design will fulfil the UR. If this not possible, the aspects of the design which are no longer appropriate must be reviewed and modified to meet the new site conditions/risk assessment.

Where the SDS has been developed by the customer or their representatives, these should be provided to the installer to review prior to the start of the installation process.

8.2 Access to shared networks

Permission must be gained from the customer/system owner prior to the connection of any external devices, such as laptops and memory sticks, to shared networks.

Where relevant, external devices must either have the latest anti-virus software and updates loaded or have been scanned using the latest anti-virus software.

8.3 Documenting changes *(BS EN 62676-4 Clause 15.2)*

Change to site plans, installation plans, system designs and/or system architecture must be agreed with the customer and annotated on the SDS.

8.4 Power requirements

Power supplies, including PoE switches and injectors, must be capable of meeting the largest load likely to be placed upon them under normal operating conditions.

Power supplies must be located within a secure area or in a position safe from tampering and must be installed in accordance with manufacturer's requirements.

All equipment housings containing mains voltages must be clearly marked.

8.5 Cable installation

Attention is drawn to the Regulations for Electrical Installations, BS 7671, also known as the IET Wiring Regulations.

All wiring and connections, including coaxial and fibre optic joints and splices, must be installed in accordance with manufacturer's requirements.

Extra-low voltage and signalling cable must not be installed in ducting/trunking which is carrying mains cable or parallel to mains cables unless suitably screened, insulated and/or segregated.

Wherever possible, extra-low voltage cables must not be brought into any item of equipment through the same entry point as mains cables.

Fixed interconnection cables must be supported by appropriate fixings, trunking or ducts.

Plastic or PVC component used as part of the installation of cables must be suitable for the environment in which it is installed.

Cables carrying data and other level signals/voltages must be of a type and size compatible with the rate of data transfer, anticipated levels of electrical interference and any voltage drop.

Where you are responsible for the installation of the network, data cabling must at a minimum be tested for the correct wire mapping (including split pairs), short and open circuits, cross talk, attenuation and speed. The results of this testing must be documented.

Cables, connectors, patch panels, termination blocks and outlet sockets must be compatible, i.e., Cat 5e and Cat 6 components and cables should not be mixed.

Care should be taken to ensure bend radius, as defined in the manufacturer's documentation, is not exceeded.

Network interconnections over 5m in length should be made using non-stranded (solid) conductors.

Network devices should be connected to interconnections via patch panels or outlet sockets using stranded pre-terminated patch cables.

Cabling must be clearly and unobtrusively labelled at each termination point with source and destination identities to facilitate future maintenance and servicing. A cross-reference chart or running out diagram showing the relationship between cables and devices must be held by the installing company.

9 Test, Commission & Handover *(BS EN 62676-4 Clause 15.3)*

As part of the commissioning and handover process, an acceptance test of the system must be carried out.

9.1 Test *(BS EN 62676-4 Annex B & C)*

A system test, using a test plan developed as part of the UR/SDS and agreed with the customer, must be conducted to ensure that all expected functions and features of the system meet the UR and SDS.

Images testing can be scenario or target based. Image chain consistency of each camera should be carried out to ensure images viewed live and/or replayed and exported meet the image performance requirements in the SDS.

Detection coverage as well as cause and effect should be tested for correct coverage and response.

Broadcast and recorded audio should be tested to ensure information is clear and is broadcast over/detected from the area defined in the UR/SDS.

Network loading tests should be carried out to gauge the systems capability to operate in the worst case operational scenario, for example, all cameras active.

The user should be advised to carry out additional network vulnerability and penetration testing where risks have been identified.

Testing must cover the operational period of the system.

Image chain consistency testing should be carried out during best and worst case lighting scenarios.

Legislative requirements that affect the design of the system must be tested/assessed for compliance.

Design requirements introduced due to a Privacy Impact Assessment (coverage/masking) should assessed for compliance.

Compliance with data protection requirements/policies should be assessed.

Compliance with local and national planning legislation should be assessed

Compliance with Display Screen Equipment (Health and Safety) legislation should be assessed, where you undertake control room design.

All results must be documented.

Documentation should include details of tests carried out and evidence captured (for example, operator acceptance checks, reference stills and videos, configuration files, network load statistics, penetration test reports, etc.) to confirm the system meets the UR/SDS.

9.2 Commissioning

A formal commissioning process must include a demonstration of the capability of all system components to the customer to enable a decision to be made on the ability of the system to meet the UR/SDS.

This may process may be carried out as well as or as part of the system test.

Additionally a physical inspection must be carried out to check the security and correct installation of all system components (including system interconnections).

The results of this inspection must be documented. See Appendix D.

9.3 Handover

A formal handover of the system must be carried out with the customer/customer's representative present.

Operator training must be carried out as agreed with the customer.

9.4 System security

Unless otherwise agreed in writing with the customer, all system accounts used by you must be deleted or locked and the user advised to change passwords when the system is handed over. This includes removing remote access rights to the system.

10 Documentation *(BS EN 62676-4 Clause 14 & 16)*

For each system, the following documentation must be retained by you and provided to the customer.

10.1 Customer documentation

The following documentation must be provided to the customer:

- Risk assessment, unless carried out by the customer (may be included as part of the UR or SDS) *(BS EN 62676-4 Clause 14.2)*.
- UR, unless produced by the customer (may be included in the SDS) *(BS EN 62676-4 Clause 14.3)*.
- SDS unless produced by the customer (should be signed by the customer) *(BS EN 62676-4 Clause 14.4)*.
- As fitted documentation.

  This can be a marked up and amended copy of the SDS.
- Test plan (this may be included in the SDS) and commissioning results *(BS EN 62676-4 Clause 14.6)*.
- The results of testing provided to the customer must at a minimum include reference images from each of the cameras at representative illumination levels throughout the operational period defined in the UR.
- Operating instructions/manuals (these should be in a format agreed with the customer) *(BS EN 62676-4 Clause 16.3)*.
- System account details and passwords *(BS EN 62676-4 Clause 16.3)*.
- System logbook.
- Handover checklist (signed by the customer and the individual handing the system over). See Appendix E.
- Certificate of acceptance (this may be included as part of the handover checklist). See Appendix E.
- NSI Certificate of Compliance.

The provision of additional information, such as full test plans and network design and configuration documentation, should be agreed with the customer.

10.2 Installer documentation

In addition to copies of the customer documentation, you must retain a full set of test results for the system.

11 Maintenance *(BS EN 62676-4 Clause 10)*

Where preventive and/or corrective maintenance service is provided, it must be in accordance with this code of practice.

11.1 Staff

You must have sufficient technicians to maintain and service all your installations in accordance with this code of practice (or other applicable technical standards including manufacturer's instructions).

11.2 Access to shared networks

Permission must be gained from the customer/system owner prior to the connection of any external devices, such as laptops and memory sticks, to shared networks.

Where relevant, external devices must either have the latest anti-virus software and updates loaded or have been scanned using the latest anti-virus software.

11.3 Corrective maintenance

The emergency service (corrective maintenance) facility must be so located and organised that, under normal circumstances, the company's technician attends the premises within the time agreed in the contract with the customer.

A reliable system of communication between the security company's operational base, the customer and all technicians must be maintained at all times.

There must be one or more stand-by technicians. If there is only one technician on call, there must be means to call out additional technicians should the need arise.

Technicians and other duty engineering staff must be available and must keep in regular and frequent contact with their operational base.

The technician must determine the cause of any fault and then carry out one or more of the following:

a) Repair and leave the system fully operational.

b) Temporarily repair the system subject to the approval of the customer.

c) With the customer's approval, disconnect part of the system and obtain the customer's signature.

d) In the case of a fault in a video transmission system, to confirm the condition and change the system to alternative transmission (if installed) and obtain the customer's signature.

If the fault on the system cannot be located or positively confirmed, the technician must contact the security company for instruction.

A report of all action taken must be made on the corrective maintenance report and the customer's signature obtained. A copy is to be left with the customer or be provided to them within 10 working days or other timeframe as agreed with the customer. See Appendix F.

Any parts of the system disconnected or temporarily repaired must be recorded, obtaining the customer's authority, and be reported for further action. The company must ensure that action is taken as soon as possible and, in any case, in accordance with the contract for maintenance.

11.4 Preventive maintenance

Frequency and types of preventive maintenance activities must reflect the equipment manufacturer and installer's recommendations.

The frequency of preventive maintenance visits should, if maintenance is carried out, meet these requirements.

Maintenance documentation should include details of how licenses and software and firmware patches and updates are to be managed.

Some maintenance tasks may be carried out by the operator or system owner.

When carrying out a preventive maintenance visit, the technician must first establish with the customer whether there have been any problems with the system since the last preceding preventive maintenance visit.

The technician must examine the system documentation, or the one kept by the customer, to see whether there have been any service calls or incidents since the last preceding routine visit.

The technician must ensure that the customer (or the customer's representative) is still fully conversant with the operation of the system.

The system must be visually inspected, checking the following items. See Appendix G:

a) The number and type of cameras, detectors and illumination are in accordance with that stated in the specification and any amendment. Draw the customer's attention to any deviations found.

b) Indicators are working correctly.

c) Signage, including warning labels, is still in place.

d) All cables and conduits (including those that are flexible) are properly supported, undamaged and showing no signs of wear.

e) Ensure sound physical fixings of all equipment including examinations for loosening or corrosion of supports and fixings, including towers and brackets. Lubricate tower mechanisms, where applicable, in accordance with manufacturer's instructions and repair or replace brackets as necessary.

f) All glands and seals on external equipment. Repair or replace as necessary to maintain the agreed specification.

g) Protection against climbing, tampering or vandalism is still in place and remains effective.

The system must then be functionally inspected, checking the following items:

a) The image quality of each camera and correct display selection. Note signs of condensation on windows of camera housings and reduction in image contrast.

b) Where necessary, remove covers and housings and clean interiors.

c) All camera functions comply with specification (for example pan, tilt, zoom, electronic iris, focus, wipers, washers, heaters, etc.) and that camera movement and fields of view are free from obstruction.

d) Operation of all display, record, store and network equipment (including time and date information) is satisfactory.

e) Function of all interfaces with alarms and detectors is satisfactory, including correct triggering of alarms.

f) Operation of supplementary illumination is satisfactory.

Illumination sources should be replaced at frequencies recommended by manufacturers so as to minimise the possibility of failure between preventive maintenance visits.

Items requiring attention must be rectified and/or reported as necessary, recording all such work on the preventive maintenance report.

Check that the performance of the system(s) continues to meet the agreed specification/UR and any periodic test scheme agreed with the customer.

Appendix A Sample risk assessment (informative)

Areas	Subjects for consideration	Detail	Site Survey annotated (YES/NO)
Targets *(with suggested image categories)*	*Individuals involved in carrying out personal attacks (identify/recognise)*		
	Individuals involved in the theft of goods, cash, data, intellectual property (identify/recognise)		
	Individuals involved in anti-social behaviour and/or vandalism (detect, observe, identify and/or recognise)		
	Environmental risks to individuals (monitor, detect and observe)		
	Crowd control and staff safety (monitor, detect and observe)		
	Control of entry (identify/recognise individuals)		
Location	*Urban, suburban or rural area*		
	Prevailing environmental conditions		
	Existing security arrangements		
	Construction of property		
Occupancy	*Hours of occupancy of areas where risks have been identified*		
	Public access to risk areas		
History of criminality in area	*Prevalence of any particular criminal activities*		
	Methods of attack		
Threats to system operation	*Damage to/theft of system components*		
	Deliberate interference to system components(moving/blinding cameras)		
	Loss of power		
	Loss/lack of illumination		

Appendix B Site survey (informative)

Surveyor	
Date & Time	
Location	

Where the site survey is carried out by the security company, the following must be documented:

- Drawings and/or photographs and/or notes of the proposed location, including details of target and risk locations.
- Notes on the approximate distances to target and risk areas (to aid camera and lens selection).
- Candidate locations for system components.
- Details of existing illumination.
- Local environmental concerns that may affect the design (foliage, vehicle parking, adjacent public and private property boundaries, etc.)
- Availability of communications and power.
- Any restrictions on site access and Health & Safety concerns.

Appendix C Technical description of image categories (normative)

Image categories

Percentages indicated in Table 1 refer to the image of a 1.7 m tall human figure as viewed on a number of screen resolutions. An increase or decrease in resolution will modify the required percentage of screen.

Alternatively, image category to screen resolution can be calculated by pixels per mm.

Example: For the image category recognise (8 mm per pixel) on a standard target of 1.7 m (1700 mm) on a 1080p (1080 pixel height screen) 1700/8 = 210 pixels, which is approximately 20% of screen height.

Monitor: A figure should typically occupy a minimum of 80 mm per pixel.

An observer should be able to monitor the number, direction and speed of movement of people across a wide area.

Detect: A figure should typically occupy a minimum of 40 mm per pixel.

When alerted, an observer should be able to search the display screens and ascertain whether a person is present or not.

Observe: A figure should typically occupy a minimum of 16 mm per pixel.

An observer should be able to see some characteristic details of the individual, such as distinctive clothing, whilst the view remains sufficiently wide enough to allow activity surrounding an incident to be monitored.

Recognise: A figure should typically occupy a minimum of 8 mm per pixel.

At this level of detail, an observer should be able to say with a high degree of confidence whether or not an individual shown is the same as someone they have seen before.

Identify: A figure should typically occupy a minimum of 4 mm per pixel.

Picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.

The above terms are included in BS EN 62676-4:2015 Clause 6.7.

Typical image height in percentage figures for common screen resolutions											
Format	**PAL**	**4K**	**1080p**	**720p**	**WSVGA**	**SVGA**	**4CIF**	**VGA**	**2CIF**	**CIF**	**QCIF**
Category											
Identify	100	20	40	60	70	70	70	85	150	150	300
Recognise	50	10	20	30	35	35	35	45	70	70	150
Observe	25	10	10	15	20	20	20	25	35	35	70
Detect	10	10	10	10	10	10	10	10	15	15	30
Monitor	5	5	5	5	5	5	5	5	10	10	15

Table 1 Typical image height in percentage figures for common screen resolutions

Appendix D Physical commissioning checks (normative)

Commissioning Technician	
Location	

Physical checks	Pass / Fail / Comments
Cable marking correct	
Cables, terminations and connections secure	
Network cable measurements complete and documented	
Protective trunking and ducts in place and secure	
Glands and grommets in place and secure	
Physical guards protecting against tamper and vandalism secure	
Anti-climb measures in place and effective	
Power, signal and data cabling suitably segregated and insulated	
External components protected against water and dust ingress	
Cabling around articulated and moveable points on masts and towers protected during movement	
Warning signage and labels provided secure, visible and accurate	

Appendix E Handover & acceptance certificate (normative)

Handover & acceptance certificate	
Company representative	
Company name	
Company address	
Telephone no	
Email	
Customer name	
Customer address	
Job/Contract no	
System record reference	
Date	

Security company handover checklist	Comments
All system documentation is correct.	
Designated operator(s) have been trained in the correct operation and maintenance of the system.	
A system log book has been provided to the customer and an explanation has been given on how to record / report events.	
All aspects of the operation of the system(s) and compliance with the UR have been demonstrated to the customer in accordance with the agreed system test specification.	
Reference images obtained during the test and commissioning process have been provided.	

Correct documentation has been given to the customer to enable the system to be correctly operated.	
Check that all documentation in accordance with NCP 104 is correct.	
The management and use of all means to access the systems applications and operating systems, including any permissions to remotely access the system, have been implemented as agreed with the customer.	
Operator(s) have been made aware of the procedure for summoning assistance in the event of system malfunction.	
Obtain customer's signature acknowledging acceptance of the system(s)	
Check that all surplus materials and equipment are cleared from the site and that premises are left clean and tidy.	

Customer acceptance certificate

I confirm that the CCTV system has been installed to my satisfaction and that the premises have been left in a tidy condition and that I have received:

- training in the operation and adjustable features of the CCTV system;
- a record book (system log book) for the CCTV system;
- a demonstration showing compliance of the CCTV system with the UR using the agreed system test specification;
- full and comprehensive written operating instructions for the CCTV system;
- details of the procedure for summoning assistance in the event of system malfunction.

Signatures and dates required	Signature	Date
Customer		
Security company		

Appendix F Corrective maintenance (informative)

F.1 Sample corrective maintenance form

Company name					
Address					
Telephone no.		Fax no.			
CORRECTIVE MAINTENANCE REPORT					
Customer		Date		Contract no.	
Address		Specification no.		Account no.	
		Location of fault			
Tel no.		Fax no.			
Reason for call-out					
1. Customer related					
A. Operator ☐	**B.** Unauthorised adjustment ☐	**C.** Unauthorised removal of equipment ☐			
D. Power fail ☐					
2. Company related					
A. Design ☐	**B.** Installation ☐	**C.** Maintenance ☐	**D.** Comms fail ☐		
E. Power fail ☐	**F.** Non-electric (for example mounting) ☐				
3. Other					
Please state					
Report/Action taken					
Further action required					
The system was left in full working order apart from the items and/or disconnections listed below:					
Technician's signature		Office use:			
		Time			
		Initials			
Customer's signature					

Appendix G Preventive maintenance (normative)

G.1 Sample preventive maintenance form

PREVENTIVE MAINTENANCE REPORT			
Customer			
Address			
Item	**Check**	**Tick**	**Remarks**
1	Check the number and type of cameras, including lenses, are in accordance with the specification and any amendment.	☐	
2	Check indicators are working correctly.	☐	
3	Check warning labels are still in place.	☐	
4	Check all cables and conduit are properly supported, undamaged and showing no signs of wear.	☐	
5	Check for sound physical fixings of all equipment including loosening or corrosion of supports and fixings including towers and brackets.	☐	
6	Check all glands and seals on external equipment.	☐	
7	Check the image quality of each camera against the reference images obtained during commissioning and the correct selection and configuration of monitors.	☐	
8	Covers and housings have been removed and interiors cleaned where necessary.	☐	
9	Check all automatic and remote control camera functions are satisfactory and that camera movement and fields of view are free from obstruction.	☐	
10	Operation of all monitoring, switching, recording and store equipment is satisfactory.	☐	
11	Function of all interfaces with alarms is satisfactory including correct triggering of alarms.	☐	
12	Operation of supplementary lighting is satisfactory.	☐	
13	Data retained meets the system data retention policy	☐	
14	Audit logs are functioning correctly	☐	
15	All system software and firmware patches and upgrades are up to date	☐	
16	Check that the performance of the system(s) continues to meet the agreed specification / UR according to the periodic test scheme agreed with the customer.	☐	
The system has been left in full working order apart from the items listed below: Items not completed at the time of the check will be completed within ..... days of the date shown below.			
Time arrived		Time left	
Technician's signature		Date	
Customer's / Customer Representative's Signature			